ALASKA PIONEER HOME		**P&P No: 09.01**
Title: HIPAA Security Rule		**Approval:** D. COTE
Key Words: Security Rule, Privacy Rule, ePHI, DSM, Contingency Plan, Training		
Team: All employees	**Effective Date: 8/1/12**	**Page: 1 of 6**

PURPOSE

To explain the purpose and process of the HIPAA Security Rule when handling Alaska Pioneer Home (AKPH) resident protected health information.

POLICY

AKPH employees use the HIPAA compliant DSM (direct secure messaging) system to encrypt emails and email attachments that contain personal health information (PHI).

DEFINITIONS

HIPAA Security Rule deals with Electronic Protected Health Information (EPHI). It names three types of security safeguards required for compliance: administrative, physical, and technical. For each type, the Rule identifies security standards, and for each standard, it names both required and addressable implementation specifications.

HIE (health information exchange) is the mobilization of healthcare information electronically across organizations within a region, community, or system.

PROCEDURE

I. HIPAA (Health Insurance Portability and Accountability Act)

A. HIPAA history and content
   1. United States Congress passed the HIPAA in 1996.
   2. Parts of the HIPAA:
      a. Title I (portability) protects health insurance coverage for workers and their families when they change or lose their jobs.
      b. Title II (accountability), known as the Administrative Simplification provision, requires that standards for electronic health care transactions and identifiers be used.
         1) The federal government has issued 5 rules under Title II:
            a) Privacy Rule
            b) Transactions and Code Sets Rule
            c) Security Rule
            d) Unique Identifiers Rule

e) Enforcement Rule

2) The standards improve the nation's health care system by increasing the use of electronic data interchange.

3) Standards apply to covered entities which include health care provider, health plan, or health care clearinghouse. Entities can range from the smallest provider to the largest, multi-state health plan.

B. Security Rule

1. The core objective is for all covered entities, such as pharmacies, hospitals, health care providers, clearinghouses, and health plans to support the confidentiality, integrity, and availability of electronic protected health information (ePHI).
2. ePHI is electronic health information *plus* any identifier which indicate an individual associated with the information (see 18 personal identifiers listed in F-7 below). The Security Rule complements the Privacy Rule.

a. The Privacy Rule pertains to all Protected Health Information (PHI) and includes verbal, written, and electronic information.

b. The Security Rule deals specifically with electronic PHI.

c. Three types of security safeguards are required for compliance with the rule:

1) Administrative safeguards are policies and procedures to clearly show how the entity will comply with the act.

2) Physical safeguards provide measures to protect the information, buildings, and equipment from natural environmental hazards and unauthorized intrusion.

3) Technical safeguards control access to computer systems and protect communication which is transmitted over open networks from being intercepted by anyone other than the intended recipient.

a) Employee log on, password, and access safeguard determines the type of information available to that employee.

b) Passwords should never be shared.

c) Effective passwords are at least 8 characters long, a combination of letters, numbers, and symbols, and difficult to guess.

C. Methods to secure ePHI

1. Organizations use different methods to secure ePHI.
2. Data is encrypted and stored on devices purchased by the State.
3. Security risks:

a. Taking information home to finish work exposes ePHI to loss or disclosure.

b. Portable media can be lost or stolen.

   c. Viewing unsafe web sites, downloading information, and surfing the net can be a security risk.
   d. Sharing data with other laptops.

D. Protected Health Information (PHI)
   1. Any oral or recorded information that is created, stored, transmitted, or received by a health provider, plan, authority, employer, insurer, school, or clearinghouse.
   2. PHI includes any health information that is identified to an individual.
      a. Data is linked to an identifier; PHI=health information +identifier.
      b. List of 18 identifiers below.
   3. Relates to the past, present, or future physical or mental health or condition of an individual.
   4. Relates to the past, present, or future payments for provision of health care.
   5. Employee records held by an employer in a covered entity are excluded.

E. Personal Information is PHI
   1. Personal information is sent by DSM within and outside the State email system.
   2. Personal information is encrypted, and consists of the individual's name plus one or more other pieces of information, such as:
      a. Social security number
      b. Driver's license number
      c. Account number
      d. Password
      e. Access code

F. DSM (direct secure messaging)

   1. The HIT (health information technology) Program office in coordination with AeHN (Alaska eHealth Network) has set up Direct Secure Messaging (DSM).
   2. DHSS procured DSM, a secure email and file transfer service which meets HIPAA requirements for protected health information (PHI) through data encryption.
   3. DSM has advantages because it encrypts both the message body and any attachments which contain PHI and other sensitive data.
   4. DSM users are validated and have been assigned a specific DSM email address. This assures that the individual on the receiving end of the message is also a HIPAA covered entity.
   5. DSM improves speed and security of information exchange while reducing potential transmission errors.

6. Alternatives to DSM such as mail, courier, and fax can be used for exchange with non-participating entities.
7. PHI is recorded information in any format, such as oral, written, or electronic, regarding the physical or mental condition of an individual, health care provision, or health care payment *plus* any of the 18 identifiers listed below.
   a. Name
   b. Telephone number
   c. Fax number
   d. Email address
   e. Social security number
   f. Medical record number
   g. Health plan beneficiary number
   h. Account number
   i. Certificate or license number
   j. Device identifiers and serial numbers
   k. Biometric identifiers, such as fingerprints and voiceprints
   l. URL address
   m. IP address
   n. Geographic subdivisions smaller than a state
   o. Individual's dates, such as birth date, admission or discharge date
   p. Vehicle identifier, serial number, license plate number
   q. Full-face photo or image
   r. Any unique identifier, number, characteristic, or code
8. DHSS employees who email files and messages containing sensitive information, either within the Home, AKPH division, DHSS department, or outside the department, must use DSM.
   a. Using regular email to transfer PHI may constitute a HIPAA violation.
9. Contact the HIT office at: hss.hitinfo@alaska.gov to discuss possible uses for DSM and to create an account.
10. A directory of current DSM users and their email address can be found at: http://www.ak-ehealth.org/ under the category DSM.
11. How it works:
    a. Sign into the HIE account at alaskahie.com; enter a *User ID* and *Password*, then click *Login*.
    b. Once logged in to the HIE, the inbox can be accessed by selecting *Secure Mail* from the toolbar.
    c. A message can be selected from the list within the inbox.
    d. New messages can be created by selecting *New Email* from the toolbar.
12. Contact AeHN Help Desk at 1-800-642-1810 with questions about the DSM.

G. Protect the computer system
   1. Malicious software can disable or damage the system.
      a. Malicious software uses viruses, spyware, and activities to disrupt computer systems.
   2. Notify supervisor about unusual email or computer function.
   3. Never install unauthorized software on to the computer.

H. Disposal of ePHI
   1. There are concerns about disposal and re-use of media containing ePHI.
   2. When disposing of electronic media containing ePHI, contact the ITS help desk.
      a. This ensures that the State and DHHS policies and procedures are followed.
      b. Media includes thumb drives, tapes, and data CD/DVDs.
   3. Deleting files from electronic media does not remove the information.
   4. Do not dispose of anything containing ePHI into regular trash receptacles.

I. Contingency plan
   1. Establishes strategies for recovering access to ePHI in emergencies such as a natural disaster, power outage, or a situation that disrupts business operation.
      a. For example, fire, vandalism, system failure, and natural disaster that damages the system that contains ePHI.
   2. DHSS is required to have data backup and disaster plans to create and maintain retrievable exact copies of ePHI. This is handled by Information Technology Services (ITS).
   3. Security processes to protect ePHI are maintained during emergency mode.

J. Information and training
   1. For questions or information contact your supervisor, the Home administrator, or the AKPH Central Office. You may also contact the Department Privacy Official directly at:

Privacy Official
Department of Health and Social Services
Division of Administrative Services
Information Systems Section
PO Box 110650 Juneau, AK 99811-0650
Phone: (907) 465-2150
Fax: (907) 463-5149
Email: PrivacyOfficial@alaska.gov

2. Alaska Department of Health and Social Services (DHSS) security policies and procedures can be found at the Department Security Office SharePoint site.

HISTORY OF REVISIONS

New: 1/1/12
Revised: 1/27/12; 7/20/12; 8/21/12
Reviewed: 1/27/12

RESOURCES

http://www.hss.state.ak.us/fa/is/hipaa/
http://www.hss.state.ak.us/fa/is/hipaa/security.htm
http://www.hss.state.ak.us/fa/is/hipaa/resources.htm

ATTACHMENTS

REFERENCES

45 CFR 160-164